Presentation Title: **The Structure of Groups**

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Md. Mehedi Hasan
IT-23606
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

Title of the Presentation

The Structure of Groups

Outline

Finite Abelian Groups:

- Decomposition into cyclic subgroups.
- Fundamental Theorem of Finite Abelian Groups.

Solvable Groups:

- Definition and examples.
- Importance in group theory and applications in Galois theory.

Objectives

- Understand the decomposition of finite Abelian groups into cyclic subgroups.
- Learn the Fundamental Theorem of Finite Abelian Groups and its applications.
- Explore solvable groups and their significance in abstract algebra.
- Apply these concepts to understand the structure and classification of groups.

Finite Abelian Groups

Definition:

- An Abelian group satisfies $a \bullet b = b \bullet a$ for all $a, b \in G$.
- A finite Abelian group has a finite number of elements.

Theorem:

- Fundamental Theorem of Finite Abelian Groups:
- Every finite Abelian group G is isomorphic to a direct product of cyclic groups of prime-power order.
- $G \cong Z\_n1 \times Z\_n2 \times \cdots \times Z\_nk$, where n1, n2, ..., nk are powers of primes.

Examples:

- $Z6 \cong Z2 \times Z3$.
- $Z12 \cong Z4 \times Z3$.

Applications:

- Cryptography: Modular arithmetic in secure communication.
- Computational group theory.

Decomposition of Finite Abelian Groups

Structural Properties:

- Every finite Abelian group can be written as a direct product of cyclic groups.

Invariant Factor Decomposition:

- $G \cong Z\_d1 \times Z\_d2 \times \cdots \times Z\_dk$, where $d\_i \mid d\_(i+1)$.

Elementary Divisors Method:

- Group decomposes as $G \cong Z\_p1\text{^}e1 \times Z\_p2\text{^}e2 \times \cdots$, where p_i are primes.

Visual Example:

- Decompose Z12: $Z12 \cong Z4 \times Z3$.

Solvable Groups

Definition:

- A group G is solvable if there exists a finite sequence of subgroups:
- $\{e\} = G0 \triangleleft G1 \triangleleft \ldots \triangleleft Gn = G$, where each G_(i+1)/G_i is Abelian.

Key Properties:

- Subgroups of solvable groups are solvable.
- Quotient groups of solvable groups are solvable.

Examples:

- Symmetric group S4 (solvable).
- Symmetric group S5 (not solvable).

Illustrative Example:

- A4: The alternating group of degree 4 is solvable.

Importance of Solvable Groups

Significance in Abstract Algebra:

- Central to Galois theory: Solvable groups determine whether polynomial equations can be solved by radicals.
- Provides a classification tool for understanding complex group structures.

Applications:

- Cryptography: Group solvability impacts algorithm design.
- Symmetry analysis in physics and chemistry.

Key Result:

- If the Galois group of a polynomial is solvable, the polynomial can be solved by radicals.

Comparative Analysis

Finite Abelian Groups vs. Solvable Groups:

Aspect:
- Finite Abelian Groups: Commutative groups with a finite number of elements.
- Solvable Groups: Groups with a solvable subgroup chain.

Key Structure:
- Finite Abelian Groups: Direct product of cyclic groups.
- Solvable Groups: Chain of Abelian quotients.

Examples:
- Finite Abelian Groups: Z6, Z12.
- Solvable Groups: S4, A4.

Applications:
- Finite Abelian Groups: Cryptography, coding theory.
- Solvable Groups: Galois theory, group classification.

Conclusion

Key Takeaways:

- Finite Abelian groups are classified by their decomposition into cyclic subgroups.
- The Fundamental Theorem of Finite Abelian Groups aids in understanding group structure.
- Solvable groups play a pivotal role in determining the solvability of polynomial equations.

Future Applications:

- Use these foundational concepts to explore advanced topics in abstract algebra, such as Galois theory and group cohomology.

References

1. Thomas W. Judson, Abstract Algebra: Theory and Applications.

Thank You